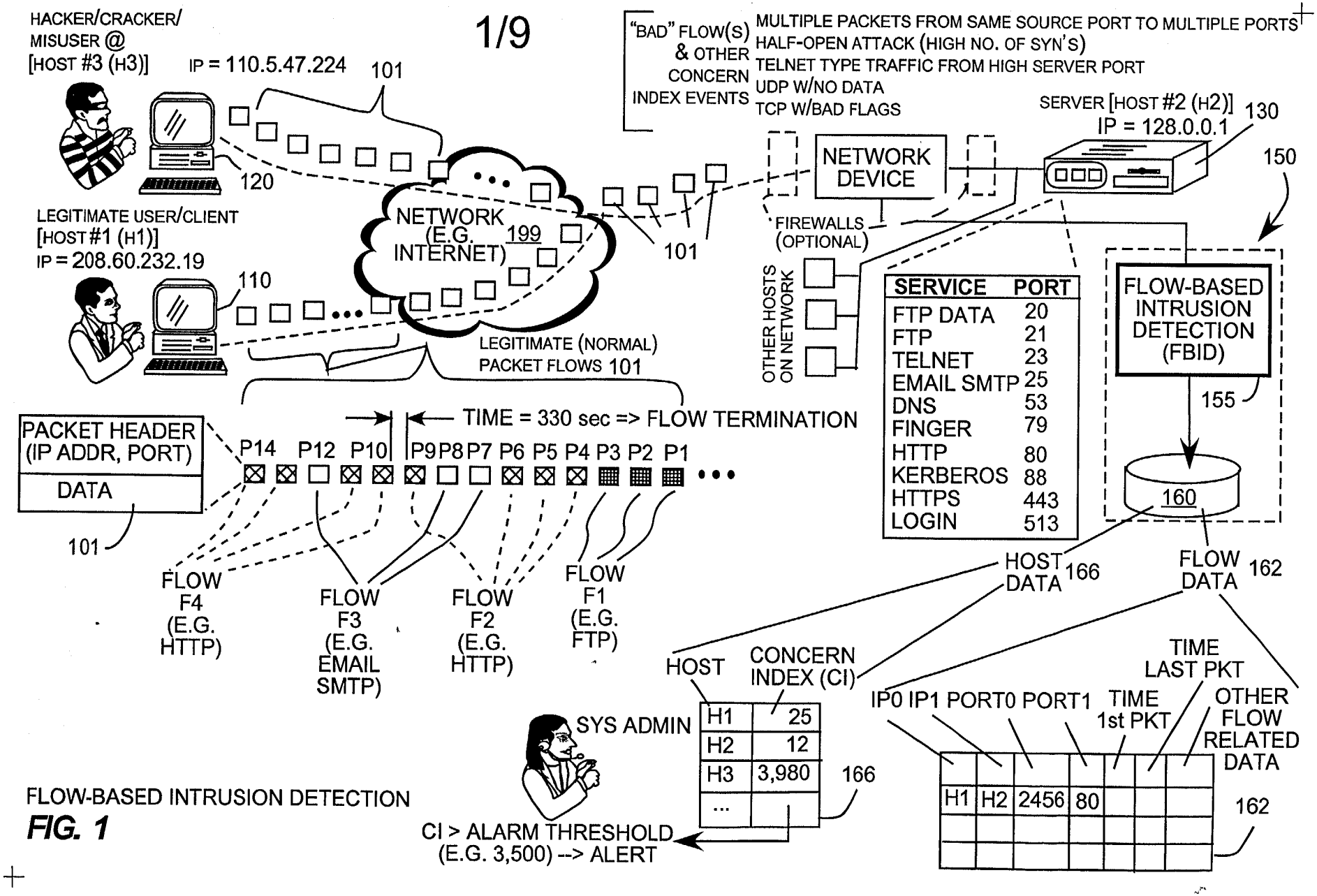
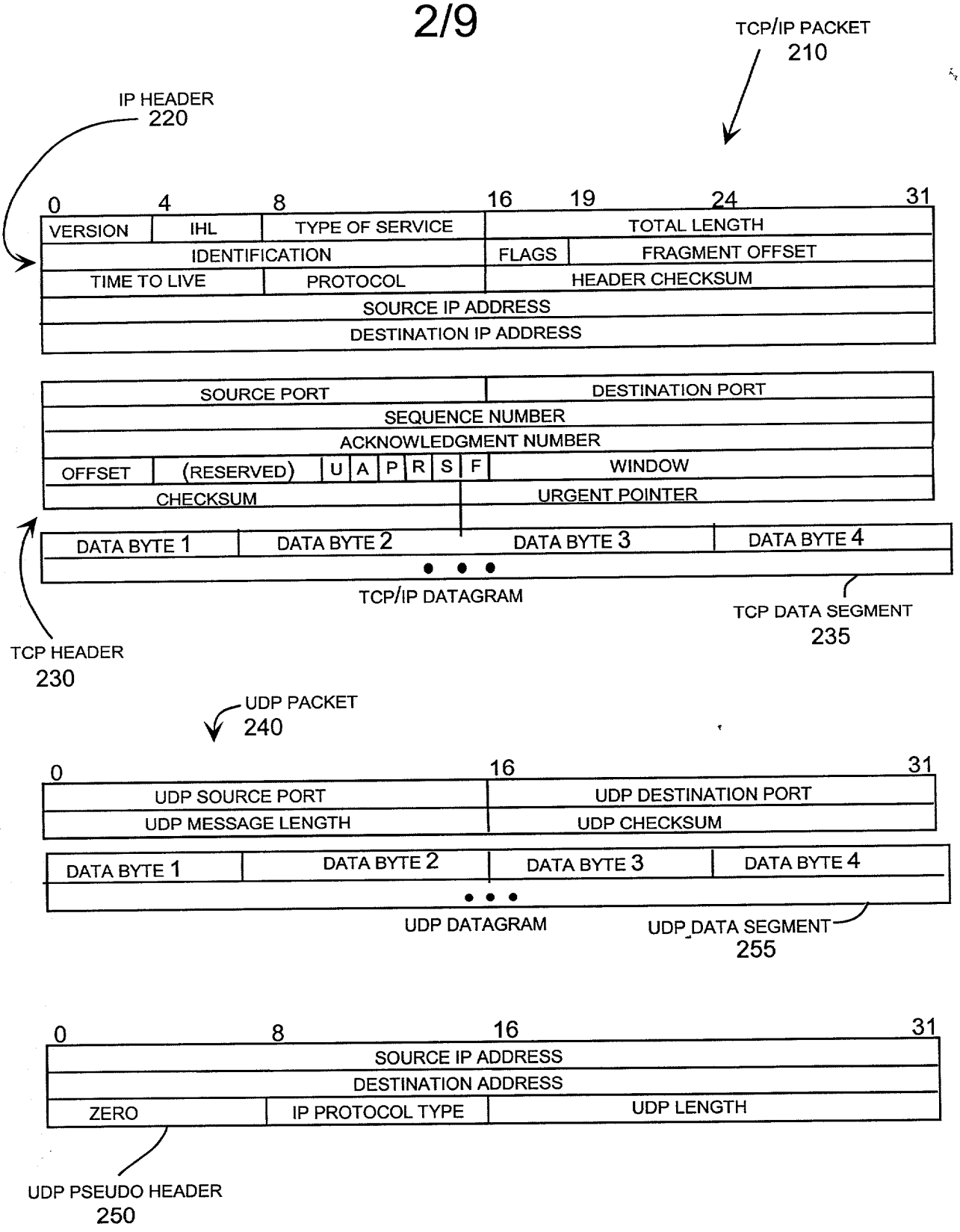


FLOW-BASED INTRUSION DETECTION

FIG. 1



PACKET HEADERS

FIG. 2

TCP/IP SESSION
300

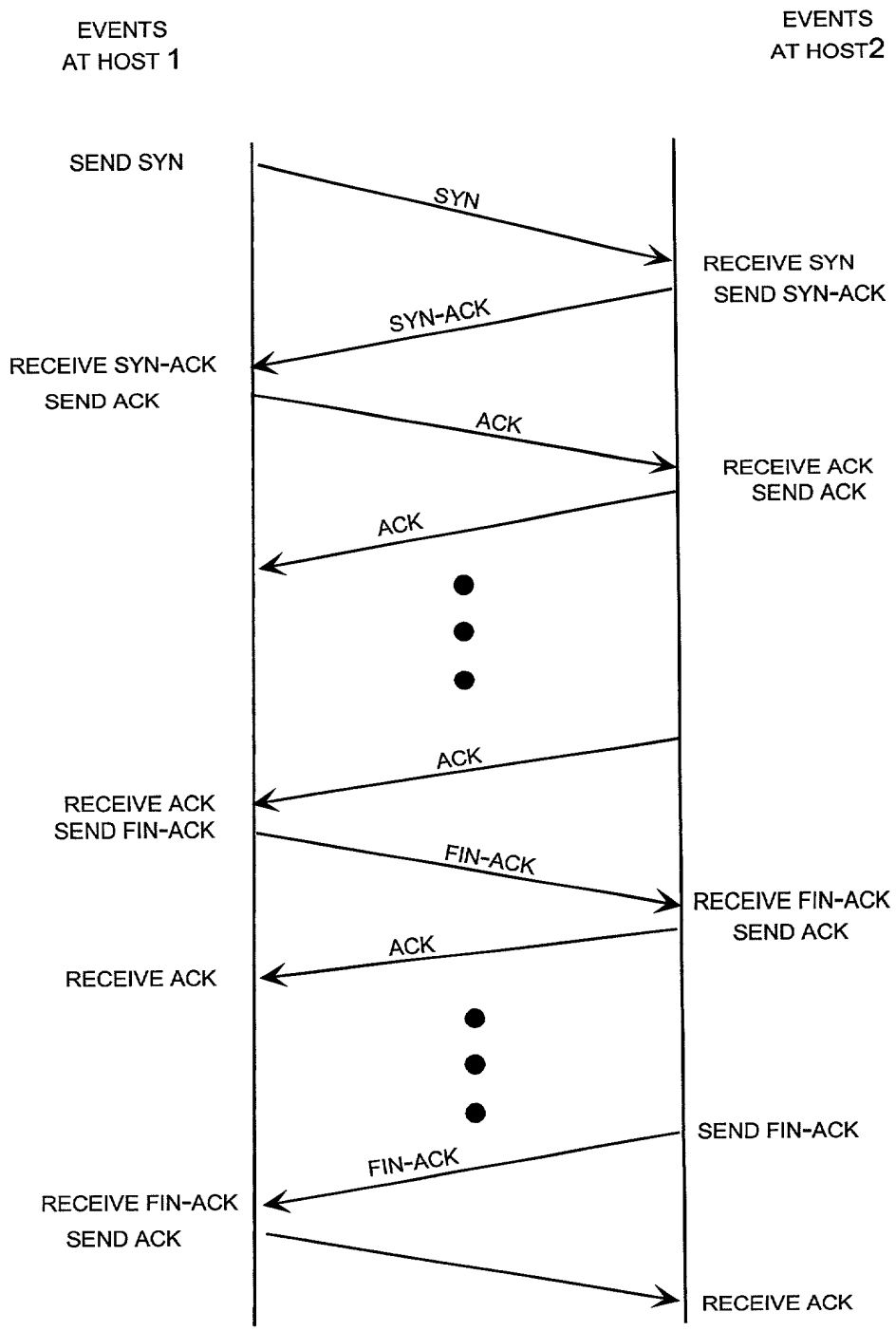


FIG. 3

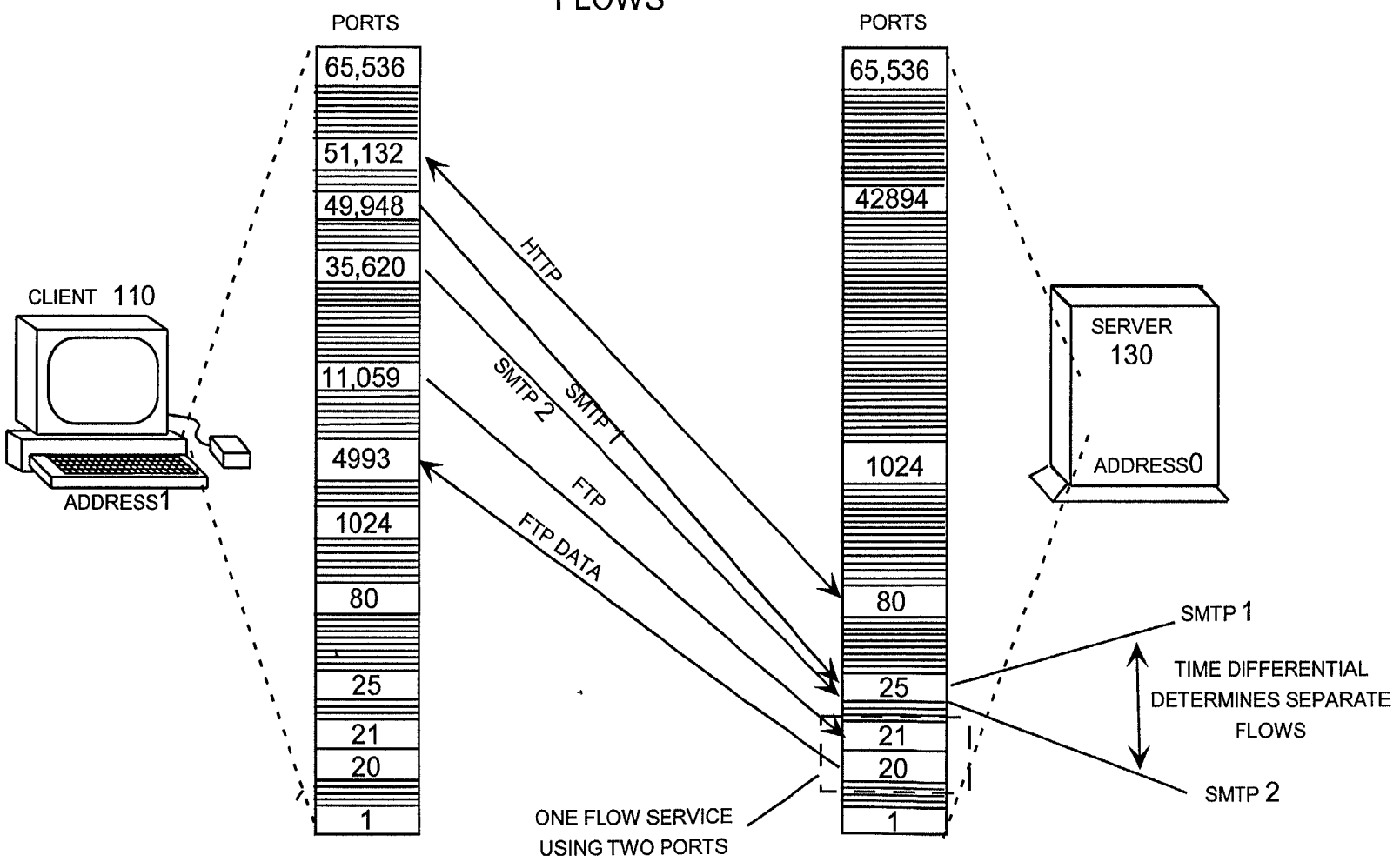
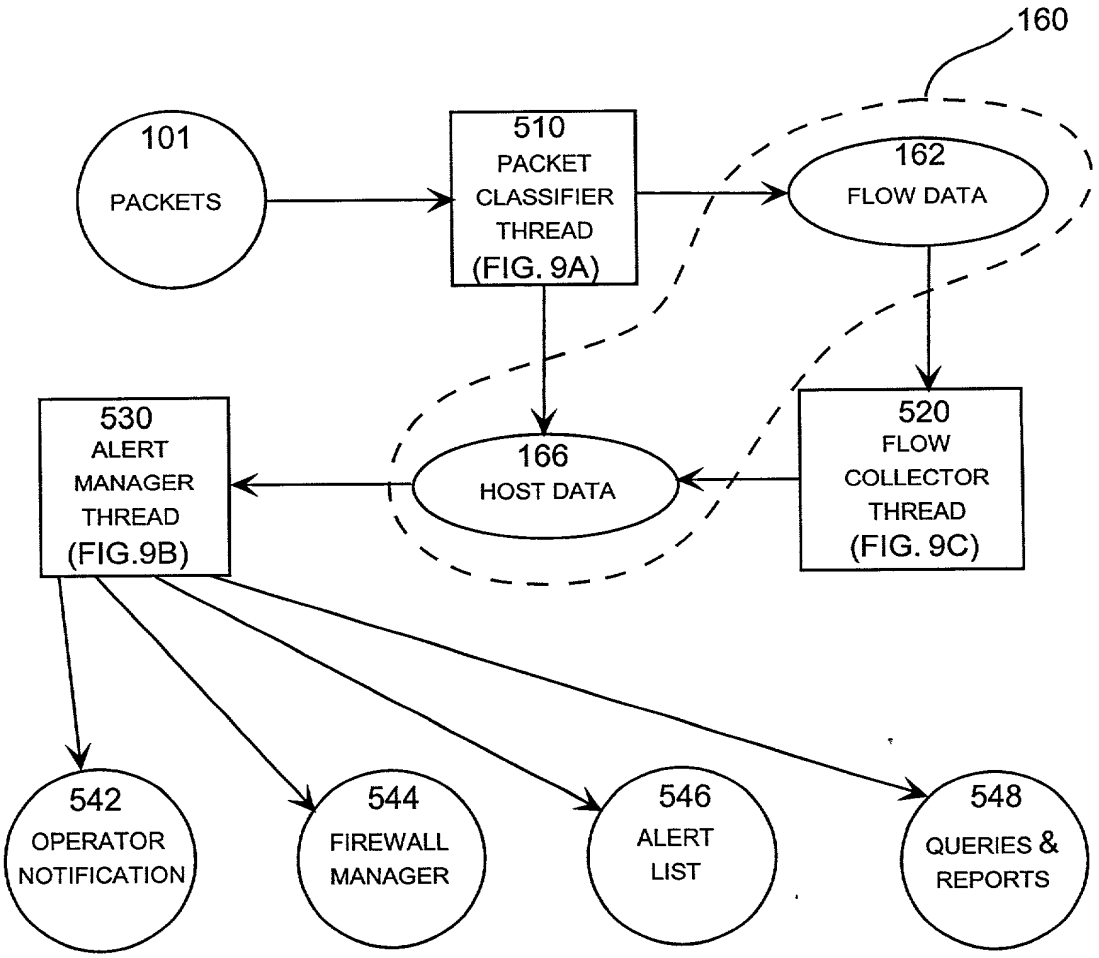

FLOWS
PORTS
PORTS
65,536
51,132
49,948
35,620
11,059
4993
1024
80
25
21
20
1
65,536
42894
1024
80
25
21
20
1
CLIENT 110
ADDRESS1
SERVER
130
ADDRESS0
HTTP
SMTP 1
SMTP 2
FTP
FTP DATA
SMTP 1
TIME DIFFERENTIAL
DETERMINES SEPARATE
FLOWS
SMTP 2
ONE FLOW SERVICE
USING TWO PORTS

FIG. 4

FLOW BASED ENGINE
155



PROGRAM THREADS: SQUARES

DATA STRUCTURES: OVALS

DATA INPUT/OUTPUT: CIRCLES

FIG. 5

TABLE I

NAME	POTENTIAL INTRUDER	RESPONSE	CI VALUE
POTENTIAL TCP PROBE	TCP PACKETS	RESET PACKETS	NUMBER OF PACKETS
POTENTIAL UDP PROBE	UDP PACKEST	ICMP PORT UNAVAILABLEPCKETS	NUMBER OF ICMP PORT UNAVAILABLE PACKETS
HALF-OPEN ATTACK	HIGH NUMBER AND RATE OF SYNS	SYN-ACKS	5000+501 PER SYN-ACK
TCP STEALTH PORT SCAN	MULTIPLE PACKETS FROM SAME SOURCE PORT TO DIFFERENT DESTINATION PORTS	RESETS	8000+1010 PER PORT OVER 4
UDP STEALTH PORT SCAN	MULTIPLE PACKETS FROM SAME SOURCE PORT TO DIFFERENT DESTINATION PORTS	NOTHING OR ICMP PORT UNAVAILABLE	8000+1010 PER PORT OVER 4

FLOW-BASED CI VALUES

FIG. 6

TABLE II

NAME	POTENTIAL INTRUDER	RESPONSE	CI VALUE
BAD FLAGS	TCP PACKET WITH UNDEFINED FLAGS		200
SHORT UDP	UDP PACKET LESS 2 DATA BYTES		200
ADDRESS SCAN	PACKETS TO MORE THAN 8 HOSTS ON SAME SUBNET	NOTHING OR RESETS	3000 PER DETECT
PORT SCAN	PACKETS TO MORE THAN 4 PORTS	RESETS	1010 PER PORT OVER 4

CI EVENT VALUES

FIG. 7

HARDWARE ARCHITECTURE

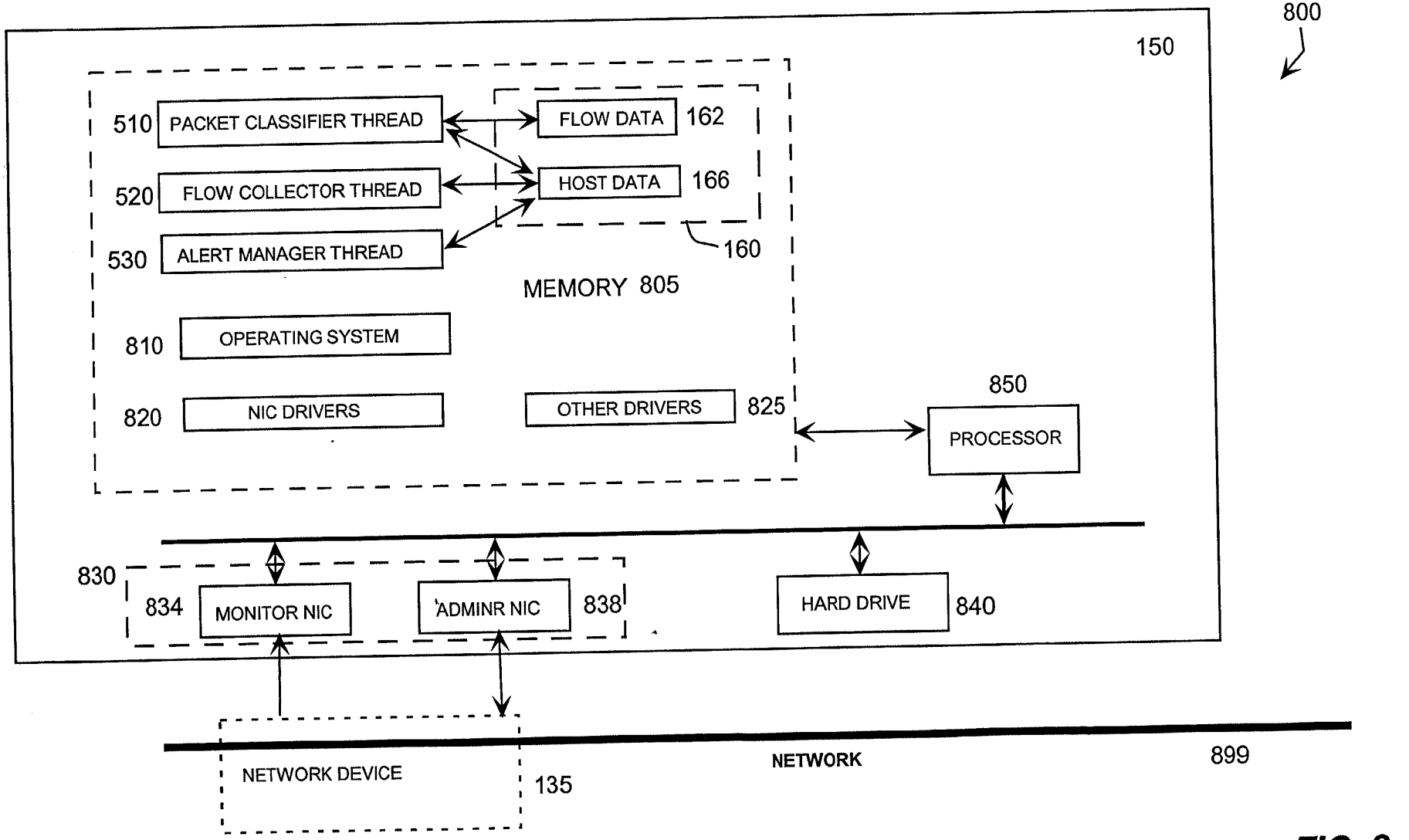


FIG. 8

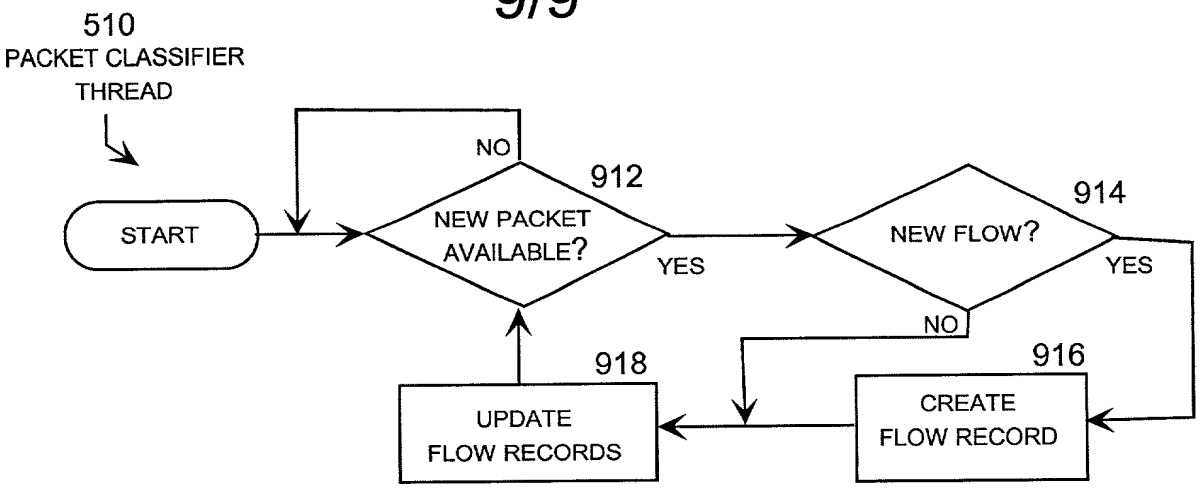


FIG. 9A

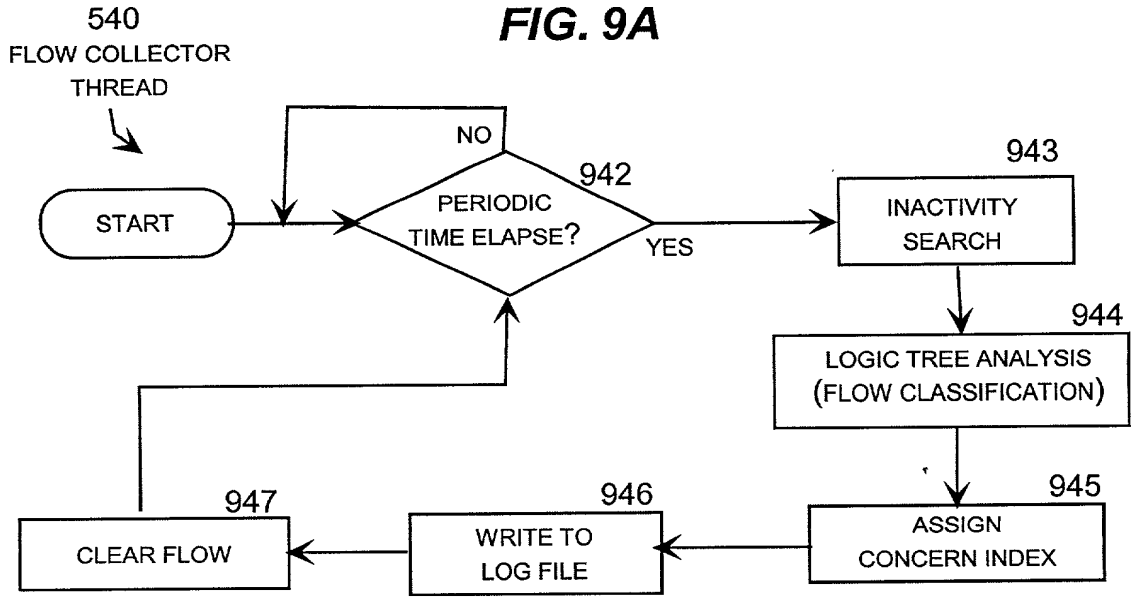


FIG. 9B

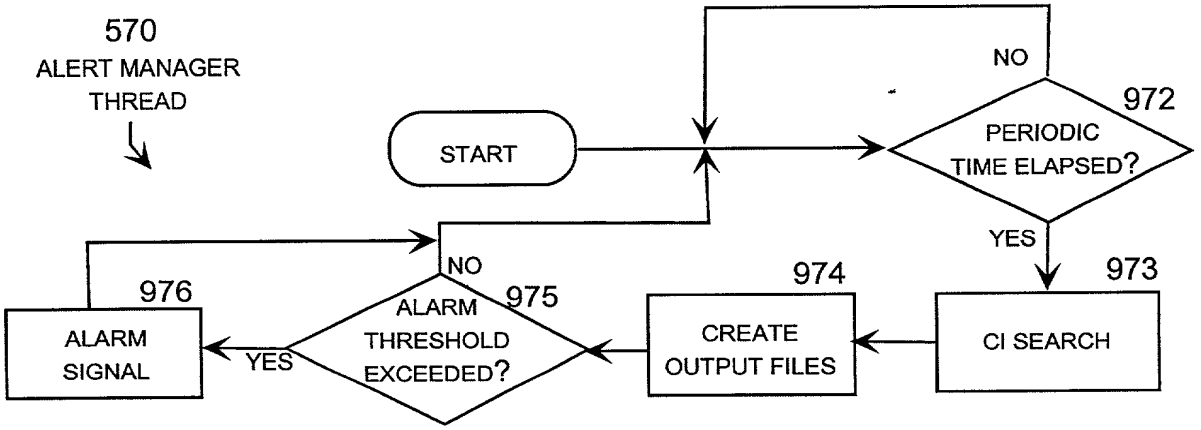


FIG. 9C